R E M A R K S

Applicant has carefully considered the Office Action of September 21, 2004 rejecting all of the claims. The present response is intended to fully address all points of objection raised by the Examiner, and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the application are respectfully requested.

Claims 1, 15 and 22 have been amended. Claims 2 to 11, 16 to 21, and 23 to 24 have been deleted. Therefore, claims 1, 12-15 and 22 remain in the case.

The present invention discloses a secure data entry peripheral device configured as a secure keyboard device in a computer system with a non-volatile storage memory for insuring secure data transmission, including transactional and credit card information, and for preventing unauthorized copying and use of software programs or packages. The inventive secure data entry peripheral device encryption technique is integrated within the device itself, and is not carried out seperately on the computer unit or devices attached by wires or add on software programs, so that each transmission of data from the peripheral device is already encrypted, giving it a high level of security with its initial transmission from the device.

Claim 1 has been amended to more clearly define the type of secure data entry peripheral device configured in the inventive process, which is a secure keyboard device, modified so as to contain an encryption unit and an electronic device capable of encrypting/decrypting and storing data entered via the keyboard device, raising the security level of the design. This is sufficiently supported by the specification at page 11, lines 11 and 12, which define the encryption unit in the secure

keyboard as the unit that performs keyboard encoding, as well as by the description of Figure 4 at page 14, fourth paragraph.

Claim 1 has also been amended to more clearly define the novelty and unobvious of the inventive device, in transmitting the processed encoded data information within the computer system as encrypted data. This is sufficiently supported by the specification at page 11, lines 9 and 10, which describes the fact that the data is sent already encrypted directly by the microcontroller associated with the secure keyboard, giving it a high security level.

The Examiner has rejected claims 1 and 22 under Sec. 102(b) as being anticipated by Clark et al.

The system described by the Clark patent is a network including plural data processing systems connected together by a communication link in a local area network, per col. 2, lines 19-48.

However, according to the present invention, the inventive data entry peripheral device encryption technique is integrated within the device itself, and is not carried out seperately on the computer unit or devices attached by wires or add on software programs, so that each transmission of data from the peripheral device is already encrypted, page 3, paragraph 3 continuing to page 4. Furthermore, the secure keyboard device has a stand-alone microcontroller having an embedded code, page 10 paragraph 4, and this is a simplified technique which cannot be considered to be disclosed by the patent to Clark. Therefore, independent claims 1 and 22 are not anticipated under Sec. 102(b).

As stated in the decision in In Re Marshall, 198 USPQ 344 (1978), "To constitute an anticipation, all material elements recited in a claim must be found in one unit of

prior art...". Since the Clark reference neither 1) identically describes the invention, nor 2) enables one skilled in the art to practice it, Applicant deems the 102(b) rejection improper, and respectfully requests that it be withdrawn.

The Examiner has rejected claims 1,3 and 12 under Sec. 103(a) as being unpatentable over Dunn et al. in view of Davis.

Dunn discloses a contact imager for reading of biometric information and smart card for processing said biometric information for presentation to the computer system.

However, according to Dunn, the smart card reader is an integral part of the biometric input device.

Davis teaches that it is desirable to share a key between two nodes and encrypt and decrypt data between the devices so as to create a secure connection, while the empowerment unit, functioning as an encryption/decryption engine, is coupled to the bus interface and the non-volatile memory through bi-directional information buses, col. 3 lines 45-50. Davis refers to an encryption unit that receives data from an input device before it is encrypted, and therefore is not applicable.

In contrast, according to the present invention regarding the secure keyboard device, the data is sent already encrypted directly by the microcontroller associated with the secure keyboard, as per the specification at page 11, lines 9 and 10. For this reason, Dunn cannot be said to render the invention obvious in combination with Davis since, as stated above, Davis is not applicable.

The Examiner has rejected claim 2 as being unpatentable over Dunn et al. in view of Davis in further view of Angelo et al. in further view of Teitelbaum et al.

Angelo describes a secure system, which can easily be bypassed by modern "Trojan horse" penetration techniques into the computer, and does not suggest a secure keyboard.

The inventive approach of having the keyboard serve as a stand alone security device is novel, since at the time of Angelo it was assumed that there is a need to protect only information that is distributed by a third party, such as a bank, credit card company, etc. It was also assumed that these third parties would distribute this information through physical devices (such as smartcards and credit cards). With the evolution of the Internet, many on-line services have been created that require the user to input a password. This method is used because it is simple and cheap.

To implement the prior art technique, including the one suggested by Angelo, it is necessary for a service provider to distribute physical 'removable data' to all their on-line clients. This would obviously be expensive, slow and not feasible as a mass market solution for the service providers. It would be uncomfortable for the clients, as well, since they would need a different physical device for each application, for example, a smartcard for online mail, one for a book retailer, etc. The prior art suggests no solution to this problem.

According to the method of the present invention, one of the uses of the device is for secure transmission of passwords. Such passwords could be initially communicated to the user through a non-Internet communication channel (phone or post), entered by the user into the secure keyboard and stored inside it in non-volatile memory. From then on, these passwords would be used as access control to on-line services in a perfectly secured manner (since the passwords would only pass through the computer in an encrypted state).

It is not apparent from Angelo how passwords are written into the 'secured memory'. It is not suggested at any point in the patent that these passwords are entered through the secure keyboard. Furthermore, it is in no way suggested that these passwords would be used for any purpose other than access to the user's own PC. No encryption means are suggested there and the secure channel described between the keyboard and 'secured memory' serves only to allow the computer to check if the password that is entered by the user matches the one in the secured memory. According to Angelo, if the result of this check is positive, then the user is issued access rights to his/her own computer.

Therefore, Angelo adds nothing to the teaching of Dunn which would render the present invention obvious.

Teitelbaum relates to a secure mouse configuration and discloses nothing regarding the inventive secure keyboard device. Therefore, Teitelbaum adds nothing to the teaching of Dunn which would render the present invention obvious.

The Examiner has rejected claim 5 as being unpatentable over Dunn et al. in view of Davis in view of Angelo et al. in view of Teitelbaum et al. in further view of Rosenberg et al.

Rosenberg relates to a mouse interface card and discloses nothing regarding the inventive secure keyboard device. Therefore, the Rosenberg patent adds nothing to the teaching of Dunn which would render the present invention obvious.

The Examiner has rejected claim 6 as being unpatentable over Dunn et al. in view of Davis in view of Angelo et al. in view of Teitelbaum et al., further in view of Brendzel et al.

Brendzel relates to incorporating a mini-keypad in the mouse and discloses nothing regarding the inventive secure keyboard device. Therefore, Brendzel adds nothing to the teaching of Dunn which would render the present invention obvious.

The Examiner has rejected claim 13 as being unpatentable over Dunn et al. in view of Davis in further view of Lee et al.

Lee teaches that a key storage device and processor should be integrated and be tamperproof to ensure the contents of the device may be read only by the authorized component and suggests nothing regarding the inventive technique of encryption/decryption integrated within a secure keyboard device. Therefore, Lee adds nothing to the teaching of Dunn which would render the present invention obvious.

The Examiner has rejected claim 14 as being unpatentable over Clark in further view of Carloganu et al.

However, the Carloganu patent teaches that a secured command interprter in a device makes it more difficult for an attacker to gain access to secrets in the device and suggests nothing, as mentioned above in the Lee patent, regarding the inventive technique of encryption/decryption integrated within a secure keyboard device. Therefore, the Carloganu patent adds nothing to the teaching of Clark which would render the present invention obvious.

It is the Applicant's position that the combination of the Clark, Dunn, Davis, Angelo, Teitelbaum, Hall, Rosenberg, Brendzel, Lee and Carloganu references to form the basis of the Sec. 103(a) rejection is improper, and Applicant respectfully requests that it be withdrawn.

Therefore, claims 1 and 22 are deemed to be patentable, and dependent claims are deemed to be patentable as being based thereon.

In citing the references under Sec. 103(a), the question is raised whether the references would suggest the invention, as stated in the decision of In Re Lintner (172 USPQ 560, 562, CCPA 1972);

> "In determining the propriety of the Patent Office case for obviousness in the first instance, it is necessary to ascertain whether or not the reference teachings would appear to be sufficient for one of ordinary skill in the relevant art having the references before him to make the proposed substitution, combination or other modification."

Similarly, In Re Regel (188 USPQ 136, CCPA 1975) decided that the question raised under Sec. 103 is whether the prior art taken as a whole would suggest the claimed invention to one of ordinary skill in the art. Accordingly, even if all the elements of a claim are disclosed in various prior art references, the claimed invention taken as a whole cannot be said to be obvious without some reason given in the prior art why one of ordinary skill would have been prompted to combine the teachings of the references to arrive at the claimed invention.

Simply put, and as stated in In Re Clinton (188 USPQ 365 CCPA 1976), "do the references themselves... suggest doing what appellants have done", such that there is a requirement that the prior art must have made any proposed modification or changes in the prior art obvious to do, rather than obvious to try.

It is respectfully put forward by the Applicant that there is no reason to consider the prior art references, Clark, Dunn, Davis, Angelo, Teitelbaum, Hall, Rosenberg, Brendzel, Lee and Carloganu, either individually or in combination, as rendering the invention obvious, since

none of them discloses a secure data entry peripheral device configured as a secure keyboard device in a computer system. The encryption unit is embedded within the device itself, so that each transmission of data from the peripheral device is already encrypted, giving it a high level of security with its initial transmission from the device.

In view of the foregoing remarks, all of the claims in the application are deemed to be allowable. Further reconsideration and allowance of the application is respectfully requested at an early date.

Respectfully submitted,

Edward Langer, Pat. Atty.
Attorney for Applicant
Reg. No. 30, 564

299698/1